REMARKS

Claims 1-81 are pending in the Application. Claims 3-13, 30-40 and 57-67 are objected to. Claims 1-81 are rejected under 35 U.S.C. §102(e). Applicant respectfully traverses these rejections for at least the reasons stated below and respectfully requests the Examiner to reconsider and withdraw these rejections.

I. CLAIM OBJECTIONS:

The Examiner has objected to claims 3-13, 30-40 and 47-67 for having a series of singular dependent claims that depend from a dependent claim separated by a claim that does not also depend from that dependent claim. Paper No. 4, page 2. Applicant has renumbered the claims, as indicated above, in accordance with the Examiner's guidelines. Applicant respectfully requests the Examiner to withdraw the objections to 3-13, 30-40 and 47-67.

II. REJECTIONS UNDER 35 U.S.C. §102(a):

The Examiner has rejected claims 1-81 under 35 U.S.C. §102(a) as being anticipated by He (U.S. Patent No. 5,944,824). Applicant respectfully traverses these rejections for at least the reasons stated below and respectfully requests that the Examiner reconsider and withdraw these rejections.

For a claim to be anticipated under 35 U.S.C. §102, each and every claim limitation must be found within the cited prior art reference and arranged as required by the claim. M.P.E.P. §2131.

Applicant respectfully asserts that He does not disclose "providing an application framework, wherein said application framework logs on a user with a first level of access in said underlying operating system" as recited in claim 1 and similarly in claims 28 and 55. The Examiner cites column 2, line 25 – column 3, line 15 of He as disclosing the above-cited claim limitation. Paper No. 4, page 2.

Applicant respectfully traverses and asserts that He instead discloses a single sign-on that allows a user to log-on only once at a user station and a security server that will, in turn, automatically log the user on to all the network elements that the user is authorized to access. There is no language in the cited passage that discloses an application framework. Neither is there any language in the cited passage that discloses an application framework that logs a user in the underlying operation system. Neither is there any language in the cited passage that discloses an application framework that logs a user with a first level of access in the underlying operation system. Thus, He does not disclose all of the limitations of claims 1, 28 and 55, and thus He does not anticipate claims 1, 28 and 55. M.P.E.P. §2131.

Applicant further asserts that He does not disclose "generating an application framework sign-on screen" as recited in claim 1 and similarly in claims 28 and 55. The Examiner cites column 2, line 25 – column 3, line 15 of He as disclosing the above-cited claim limitation. Paper No. 4, page 2. Applicant respectfully traverses. As stated above, He instead discloses a single sign-on that allows a user to log-on only once at a user station and a security server that will, in turn, automatically log the user on to all the network elements that the user is authorized to access. As stated above, there is no language in the cited passage that discloses an application framework. Neither is there any language in the cited passage that discloses an application framework sign-on screen. The cited passage does disclose the term "single sign-on" but there is no language in the cited passage that discloses a sign-on screen. Thus, He does not disclose all of the limitations of claims 1, 28 and 55, and thus He does not anticipate claims 1, 28 and 55. M.P.E.P. §2131.

Applicant further asserts that He does not disclose "entering a logon input on said generated application framework sign-on screen" as recited in claim 1 and similarly in claims 28 and 55. The Examiner cites column 2, line 25 – column 3, line 15 of He as disclosing the above-cited claim limitation. Paper No. 4, page 2. Applicant respectfully traverses. As stated above, He instead discloses a single sign-on that allows a user to log-on only once at a user station and a security server that

will, in turn, automatically log the user on to all the network elements that the user is authorized to access. As stated above, there is no language in the cited passage that discloses an application framework. Neither is there any language in the cited passage that discloses an application framework sign-on screen. Neither is there any language in the cited passage that discloses entering a login input on the generated application framework sign-on screen. The cited passage does disclose the term "single sign-on" but there is no language in the cited passage that discloses a sign-on screen or entering a login input on the sign-on screen. Thus, He does not disclose all of the limitations of claims 1, 28 and 55, and thus He does not anticipate claims 1, 28 and 55. M.P.E.P. §2131.

Applicant further asserts that He does not disclose "comparing said logon input with an application framework security database to determine level of access" as recited in claim 1 and similarly in claims 28 and 55. The Examiner cites column 2, line 25 – column 3, line 15 and column 15, lines 47-54 of He as disclosing the above-cited claim limitation. Paper No. 4, page 3. Applicant respectfully traverses. As stated above, He instead discloses a single sign-on that allows a user to log-on only once at a user station and a security server that will, in turn, automatically log the user on to all the network elements that the user is authorized to access. He further discloses a database ("DCE Registry") used to store user account and network element data. However, there is no language in the cited passages that discloses comparing login input with data stored in the DCE Registry to determine the level of access. Thus, He does not disclose all of the limitations of claims 1, 28 and 55, and thus He does not anticipate claims 1, 28 and 55. M.P.E.P. §2131.

Claims 2-27, 29-54 and 56-81 each recite combinations of features including the above combinations, and thus are not anticipated for at least the above-stated reasons. Claims 2-27, 29-54 and 56-81 recite additional features, which, in combination with the features of the claims upon which they depend are not anticipated by He.

For example, He does not disclose "selecting an indication of said first level of access" as recited in claim 2 and similarly in claims 29 and 56. Further, He does not disclose "selecting an indication of a second level of access" as recited inc claim 15 and similarly in claims 42 and 69. The Examiner cites column 4, lines 5-11 and column 5, lines 15-27 of He as disclosing the above-cited claim limitation. Paper No. 4, page 3. Applicant respectfully traverses and asserts that He instead discloses a secured network which is a network security architecture that protects accesses to a plurality of network elements. He further discloses that a user obtains access by sending a request to one or more of the network elements which goes through the network security server. He further discloses that one of the security mechanisms (authorization module) that runs on the security server determines the set of network elements an authenticated user can access. He further discloses that this access list is provided to the user once the authentication check is passed. He further discloses that the user can choose from the list the desired network element and is not even aware of the existence of the network elements that the user is not authorized to access. Hence, He discloses that the security server determines the set of network elements that a user is authorized to access. However, there is no language in the cited passages that discloses selecting an indication of a first level of access. Similarly, there is no language in the cited passages that discloses selecting an indication of a second level of access. There is no indication to be selected where the indication corresponds to either a first or a second level of access. Instead, as stated above, He discloses that the security server determines the set of network elements that a user is authorized to access. Thus, He does not disclose all of the limitations of claims 2, 15, 29, 42, 56 and 69, and thus He does not anticipate claims 2, 15, 29, 42, 56 and 69. M.P.E.P. §2131.

Applicant further asserts that He does not disclose "wherein said user is logged onto said underlying operating system and an application environment with said first level of access thereby bypassing said initial sign-on screen of said underlying operating system with said single sign-on" as recited in claim 3 and

similarly in claims 30 and 57. The Examiner cites column 2, line 25 – column 3, line 15 of He as disclosing the above-cited claim limitation. Paper No. 4, page 3. Applicant respectfully traverses. As stated above, He instead discloses a single sign-on that allows a user to log-on only once at a user station and a security server that will, in turn, automatically log the user on to all the network elements that the user is authorized to access. There is no language in the cited passage that discloses logging onto an underlying operating system and an application environment. Neither is there any language in the cited passage that discloses logging onto an underlying operating system and an application environment with a first level of access. Neither is there any language in the cited passage that discloses logging onto an underlying operating system and an application environment with a first level of access thereby bypassing an initial sign-on screen of the underlying operating system with the single sign-on. Thus, He does not disclose all of the limitations of claims 3, 30 and 57, and thus He does not anticipate claims 3, 30 and 57. M.P.E.P. §2131.

Applicant further asserts that He does not disclose "wherein if said logon input is not entitled to a second level of access according to said application framework security database, then said user is logged onto an application environment and said underlying operating system as said first level of access" as recited in claim 4 and similarly in claims 31 and 58. Applicant further asserts that He does not disclose "wherein if said logon input is not entitled to a second level of access according to said application framework security database, then an indication of said second level of access will not be generated to said user, wherein said user is restricted to said first level of access" as recited in claim 10 and similarly in claims 37 and 64. Applicant further asserts that He does not disclose "wherein if said logon input is not entitled to said second level of access according to said application framework security database, then said user is restricted to said first level of access" as recited in claim 16 and similarly in claims 43 and 70. The Examiner cites column 5, lines 15-27; column 7, lines 32-41 and column 8, lines 40-46 of He as disclosing

the above-cited claim limitations. Paper No. 4, page 3. Applicant respectfully traverses.

He instead discloses a secured network which is a network security architecture that protects accesses to a plurality of network elements. He further discloses that a user obtains access by sending a request to one or more of the network elements which goes through the network security server. He further discloses that one of the security mechanisms (authorization module) that runs on the security server determines the set of network elements an authenticated user can access. He further discloses that this access list is provided to the user once the authentication check is passed. He further discloses that the user can choose from the list the desired network element and is not even aware of the existence of the network elements that the user is not authorized to access. He further discloses a control unit, control mechanism 70, configured to grant single sign-on capability to a user to none, a subset or all of the network elements that are authorized by the network for the user to access. He further discloses the capability of password recovery by administrators called "super users."

Hence, He discloses that the security server determines the set of network elements that a user is authorized to access. He further discloses a control unit that grants single sign-on capability to a user to none, a subset or all of the network elements that are authorized by the network for the user to access. He further discloses the capability of password recovery by administrators called "super users." None of this language discloses logging a user onto an application environment and an underlying operating system as a first level of access. Neither does this language disclose logging a user onto an application environment and an underlying operating system as a first level of access if the logon input is not entitled to a second level of access according to an application framework security database. Neither does this language disclose not generating an indication of a second level of access. Neither does this language disclose not generating an indication of a second level of access if the logon input is not entitled to a second level of access according to an application

framework security database. Neither does this language disclose that the user is restricted to a first level of access. Neither does this language disclose that the user is restricted to a first level of access if the login input is not entitled to a second level of access according to an application framework security database. Thus, He does not disclose all of the limitations of claims 4, 10, 16, 31, 37, 43, 58, 64 and 70, and thus He does not anticipate claims 4, 10, 16, 31, 37, 43, 58, 64 and 70. M.P.E.P. §2131.

Applicant further asserts that He does not disclose "executing a switch user program to switch said user to said second level of access" as recited in claim 6 and similarly in claims 34 and 61. Applicant further asserts that He does not disclose "generating an indication of said second level of access" as recited in claim 11 and similarly in claims 38 and 65. Applicant further asserts that He does not disclose "executing a switch user program to switch level of access to said second level of access by selecting said indication of said second level of access" as recited in claim 12 and similarly in claims 39 and 66. Applicant further asserts that He does not disclose "executing a switch user program to switch said user to said second level of access" as recited in claim 17 and similarly in claims 44 and 71. The Examiner cites column 2, line 25 – column 3, line 15; column 5, lines 15-27; column 7, lines 32-41; column 8, lines 40-46; and column 14, line 54 – column 15, line 5 of He as disclosing the above-cited claim limitations. Paper No. 4, page 4. Applicant respectfully traverses.

He instead discloses a secured network which is a network security architecture that protects accesses to a plurality of network elements. He further discloses that a user obtains access by sending a request to one or more of the network elements which goes through the network security server. He further discloses that one of the security mechanisms (authorization module) that runs on the security server determines the set of network elements an authenticated user can access. He further discloses that this access list is provided to the user once the authentication check is passed. He further discloses that the user can choose from the list the desired network element and is not even aware of the existence of the network

elements that the user is not authorized to access. He further discloses a control unit, control mechanism 70, configured to grant single sign-on capability to a user to none, a subset or all of the network elements that are authorized by the network for the user to access. He further discloses the capability of password recovery by administrators called "super users."

Hence, He discloses that the security server determines the set of network elements that a user is authorized to access. He further discloses a control unit that grants single sign-on capability to a user to none, a subset or all of the network elements that are authorized by the network for the user to access. He further discloses the capability of password recovery by administrators called "super users." None of this language discloses executing a program to switch user to a second level of access. Neither does this language disclose generating an indication of a second level of access. Neither does this language disclose executing a program to switch the level of access to a second level of access. Neither does this language disclose executing a program to switch the level of access to a second level of access by selecting an indication of a second level of access. Neither does this language disclose executing a program to switch the user to a second level of access. Thus, He does not disclose all of the limitations of claims 6, 11, 12, 17, 34, 38, 39, 44, 61, 65, 66 and 71, and thus He does not anticipate claims 6, 11, 12, 17, 34, 38, 39, 44, 61, 65, 66 and 71. M.P.E.P. §2131.

Applicant further asserts that He does not disclose "wherein said switch user program switches said user to said second level of access by modifying an underlying operating system's registry" as recited in claim 8 and similarly in claims 13, 35, 40, 62 and 67. The Examiner cites column 5, lines 49-58 of He as disclosing the above-cited claim limitation. Paper No. 4, page 4. Applicant respectfully traverses and asserts that He instead discloses that the network logs all user access attempts, whether they are successful or not, to create an audit trail. This language is not the same as switching a user to a second level of access. Instead, He simply discloses tracking the login attempts in a log file. He does not disclose switching a user to a

different level of access. Neither is there any language in the cited passage that discloses switching a user to a second level of access by modifying an underlying operating system's registry. Thus, He does not disclose all of the limitations of claims 8, 13, 35, 40, 62 and 67, and thus He does not anticipate claims 8, 13, 35, 40, 62 and 67. M.P.E.P. §2131.

Applicant further asserts that He does not disclose "wherein said switch user program logs off said user with said first level of access, wherein said underlying operating system logs on said user with said second level of access" as recited in claim 9 and similarly in claims 14, 36, 41, 63 and 68. The Examiner cites column 2, line 25 – column 3, line 15; column 5, lines 15-27; column 13, lines 35-37; and column 14, line 54 – column 15, line 5 of He as disclosing the above-cited claim limitation. Paper No. 4, page 4. Applicant respectfully traverses.

As stated above, He instead discloses a secured network which is a network security architecture that protects accesses to a plurality of network elements. He further discloses that a user obtains access by sending a request to one or more of the network elements which goes through the network security server. He further discloses that one of the security mechanisms (authorization module) that runs on the security server determines the set of network elements an authenticated user can access. He further discloses that this access list is provided to the user once the authentication check is passed. He further discloses that the user can choose from the list the desired network element and is not even aware of the existence of the network elements that the user is not authorized to access.

Hence, He discloses that the security server determines the set of network elements that a user is authorized to access. He further discloses that the user can choose from the access list, provided to the user, the desired network element. None of this language discloses logging on a user with a second level of access by an underlying operating system. Neither does this language disclose logging off a user with a first level of access by a program. Thus, He does not disclose all of the

limitations of claims 9, 14, 36, 41, 63 and 68, and thus He does not anticipate claims 9, 14, 36, 41, 63 and 68. M.P.E.P. §2131.

Applicant further asserts that He does not disclose "comparing said logon input with an underlying operating system security database, wherein if said underlying operating system security database verifies said user with access to said second level of access, then said switch user program switches said user to said second level of access" as recited in claim 19 and similarly in claims 46 and 73. The Examiner cites column 5, lines 7-14 and column 15, lines 6-22 of He as disclosing the above-cited claim limitation. Paper No. 4, page 4. Applicant respectfully traverses and asserts that He instead discloses that a request is sent to the user station requesting a user identifier and a password. He further discloses that the user information will be checked against the information in the user profile of the central security database at the security server. There is no language in the cited passages that discloses verifying that the user has access to a second level of access. Neither is there any language in the cited passages that discloses switching the user to a second level of access. Neither is there any language in the cited passages that discloses switching the user to a second level of access if the user has access to the second level of access. Thus, He does not disclose all of the limitations of claims 19, 46 and 73, and thus He does not anticipate claims 19, 46 and 73. M.P.E.P. §2131.

Applicant further asserts that He does not disclose "wherein said switch user program switches said user to said second level of access by modifying an underlying operating system's registry" as recited in claim 20 and similarly in claims 47 and 74. Applicant further asserts that He does not disclose "wherein said switch user program logs off said user with said first level of access, wherein said underlying operating system logs on said user with said second level of access" as recited in claim 21 and similarly in claims 48 and 75. The Examiner cites column 5, lines 7-14 and column 15, lines 6-22 of He as disclosing the above-cited claim limitation. Paper No. 4, page 4. Applicant respectfully traverses and asserts that He instead discloses that a request is sent to the user station requesting a user identifier and a password. He further

discloses that the user information will be checked against the information in the user profile of the central security database at the security server. There is no language in the cited passages that discloses switching a user to a second level of access. Neither is there any language in the cited passages that discloses switching a user to a second level of access by modifying an underlying operating system's registry. Neither is there any language in the cited passages that discloses logging off a user with a first level of access by a program. Neither is there any language in the cited passages that discloses logging on the user with a second level of access by an underlying operating system. Thus, He does not disclose all of the limitations of claims 20, 21, 47, 48, 74 and 75, and thus He does not anticipate claims 20, 21, 47, 48, 74 and 75. M.P.E.P. §2131.

Applicant further asserts that He does not disclose "comparing said logon input with an underlying operating system security database, wherein if said underlying operating system security database does not verify said user with access to said second level of access, then the method further comprises the step of: requesting from said user a logon identification; and comparing said logon identification with said underlying operating system security database" as recited in claim 22 and similarly in claims 49 and 76. The Examiner cites column 5, lines 7-14; column 8, lines 40-46 and column 15, lines 6-22 of He as disclosing the above-cited claim limitations. Paper No. 4, page 5. Applicant respectfully traverses.

He instead discloses that a request is sent to the user station requesting a user identifier and a password. He further discloses that the user information will be checked against the information in the user profile of the central security database at the security server. He further discloses the capability of password recovery by administrators called "super users." He further discloses if a user without single sign-on capability wishes to access, the user is first authenticated to the security server node and a list of network elements the user is allowed to access is displayed.

While He discloses checking the user information with information stored in a profile, there is no language in the cited passages that discloses not verifying the user with access to a second level of access. Neither is there any language in the cited passages that discloses that the user is requested for logon identification, which is compared with a security database, if the user is not verified with access to a second level of access. Thus, He does not disclose all of the limitations of claims 22, 49 and 76, and thus He does not anticipate claims 22, 49 and 76. M.P.E.P. §2131.

Applicant further asserts that He does not disclose "wherein if said underlying operating system security database verifies said user with access to said second level of access, then said switch user program switches said user to said second level of access" as recited in claim 25 and similarly in claims 52 and 79. Applicant further asserts that He does not disclose "wherein said switch user program switches said user to said second level of access by modifying an underlying operating system's registry" as recited in claim 26 and similarly in claims 53 and 80. Applicant further asserts that He does not disclose "wherein said switch user program logs off said user with said first level of access, wherein said underlying operating system logs on said user with said second level of access" as recited in claim 27 and similarly in claims 54 and 81. The Examiner cites column 2, line 25 – column 3, line 15; column 5, lines 7-27; column 7, lines 32-41; column 8, lines 40-46 and column 14, line 54 – column 15, line 22 of He as disclosing the above-cited claim limitations. Paper No. 4, page 5. Applicant respectfully traverses.

As stated above, He instead discloses a secured network which is a network security architecture that protects accesses to a plurality of network elements. He further discloses that a user obtains access by sending a request to one or more of the network elements which goes through the network security server. He further discloses that one of the security mechanisms (authorization module) that runs on the security server determines the set of network elements an authenticated user can access. He further discloses that this access list is provided to the user once the authentication check is passed. He further discloses that the user can choose from the

list the desired network element and is not even aware of the existence of the network elements that the user is not authorized to access. He further discloses a control unit, control mechanism 70, configured to grant single sign-on capability to a user to none, a subset or all of the network elements that are authorized by the network for the user to access. He further discloses the capability of password recovery by administrators called "super users."

Hence, He discloses that the security server determines the set of network elements that a user is authorized to access. He further discloses a control unit that grants single sign-on capability to a user to none, a subset or all of the network elements that are authorized by the network for the user to access. He further discloses the capability of password recovery by administrators called "super users." None of this language discloses switching a user to a second level of access by a program. Neither does this language disclose switching a user to a second level of access by a program if an underlying operating system security database verifies the user with access the second level of access. Neither does this language disclose switching a user to a second level of access by modifying an underlying operating system's registry. Neither does this language disclose logging off a user with a first level of access by a program. Neither does this language disclose logging on the user with a second level of access by an underlying operating system. Thus, He does not disclose all of the limitations of claims 25-27, 52-54 and 79-81, and thus He does not anticipate claims 25-27, 52-54 and 79-81. M.P.E.P. §2131.

Applicant further asserts that He does not disclose "wherein if said underlying operating system security database does not verify said user with access to said second level of access, then said user is restricted to said first level of access" as recited in claim 24 and similarly in claims 51 and 78. The Examiner cites column 2, line 25 – column 3, line 15; column 5, lines 7-27; column 7, lines 32-41; column 8, lines 40-46 and column 14, line 54 – column 15, line 22 of He as disclosing the above-cited claim limitations. Paper No. 4, page 5. Applicant respectfully traverses.

As stated above, He instead discloses a secured network which is a network security architecture that protects accesses to a plurality of network elements. He further discloses that a user obtains access by sending a request to one or more of the network elements which goes through the network security server. He further discloses that one of the security mechanisms (authorization module) that runs on the security server determines the set of network elements an authenticated user can access. He further discloses that this access list is provided to the user once the authentication check is passed. He further discloses that the user can choose from the list the desired network element and is not even aware of the existence of the network elements that the user is not authorized to access. He further discloses a control unit, control mechanism 70, configured to grant single sign-on capability to a user to none, a subset or all of the network elements that are authorized by the network for the user to access. He further discloses the capability of password recovery by administrators called "super users."

Hence, He discloses that the security server determines the set of network elements that a user is authorized to access. He further discloses a control unit that grants single sign-on capability to a user to none, a subset or all of the network elements that are authorized by the network for the user to access. He further discloses the capability of password recovery by administrators called "super users." None of this language discloses restricting a user to a first level of access. Neither does this language disclose restricting a user to a first level of access if the underlying operating system security database does not verify the user with access to a second level of access. Thus, He does not disclose all of the limitations of claims 27, 54 and 81, and thus He does not anticipate claims 24, 51 and 78. M.P.E.P. §2131.

As a result of the foregoing, Applicant respectfully asserts that not each and every claim limitation was found within the cited prior art reference, and thus claims 1-81 are not anticipated by He.

CONCLUSION:

As a result of the foregoing, it is asserted by Applicant that claims 1-81 in the Application are in condition for allowance, and Applicant respectfully requests an allowance of such claims. Applicant respectfully requests that the Examiner call Applicant's attorney at the below listed number if the Examiner believes that such a discussion would be helpful in resolving any remaining issues.

Respectfully submitted,

WINSTEAD SECHREST & MINICK P.C.

Attorneys for Applicant

By: _____

Robert A. Voigt, Jr.
Reg. No. 47,159
Kelly K. Kordzik
Reg. No. 36,571

P.O. Box 50784
Dallas, TX 75201
(512) 370-2832

Austin_1 257920v.1